Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

A Memoir in the Theory of Numbers.

By Arthur S. Hathaway.

Part I.—*Introduction.*

1. It has seemed desirable to begin this memoir with a brief account of the labors of others in the same direction, in order that the object of the memoir and its relations to previous results may be more clearly understood.

The labors of Gauss, Kummer, Dirichlet, Kronecker, Dedekind, and others, have extended the scope of the theory of numbers far beyond its original limit of the science of the natural numbers $0, \pm 1, \pm 2, \pm 3, \ldots.$ Gauss began the extension by showing that the theory of quantities of the form $a + b\sqrt{-1}$, where a and b are natural numbers, is quite similar to the theory of natural numbers. Quantities of this form may be called *biquadratic* numbers or integers; and one biquadratic integer is divisible by another when the quotient is a biquadratic integer. The numbers ± 1, $\pm\sqrt{-1}$, like ± 1 in the theory of natural numbers, divide all biquadratic integers, and are therefore set apart as "units" or "improper divisors." Every biquadratic integer may be factored into a product of powers of non-factorable or "prime" biquadratic integers; and, disregarding possible changes of these primes by unit factors, the factoring can be accomplished in only one way. Biquadratic primes divide themselves into three classes:

(1). Natural prime numbers, as $3, 7, \ldots.$ of the form $4n + 3$.
(2). The conjugate biquadratic factors of natural primes of the form $4n + 1$.
(3). The number $1 + \sqrt{-1}$.

Following the development of the theory of biquadratic numbers came a similar development of the theory of *cubic* numbers or quantities of the form $a + bt$, where a, b are natural numbers and t is a primitive cube root of unity, viz. $t^2 + t + 1 = 0$. The cubic primes are also divided into three classes:

(1). Natural primes, as $2, 5, \ldots.$ of the form $3n + 2$.
(2). The conjugate cubic factors of natural primes of the form $3n + 1$.
(3). The numbers $1 - t$, $1 - t^2$.

It is worthy of remark, as illustrating the manner in which mathematical theories of importance often originate, that neither of the preceding theories was developed systematically and for its own sake, but that each was the result of an effort to solve the problems of *biquadratic* and *cubic reciprocity* in the theory of numbers.

Another system of quantities whose theory is well known to be similar to the theory of natural numbers is the system of rational entire functions of an indeterminate x.

2. An important feature of all these theories is the fact that Euclid's process of finding the greatest common divisor of two numbers may, in each system, be brought to an end by arriving at the remainder, zero; namely, in the system of natural numbers each remainder may be made less than the preceding one; in the biquadratic and cubic systems the *norm** of each remainder may be made less than that of the preceding remainder, and in the algebraic system the *degree* of each remainder may be made less than that of the preceding remainder.

The importance of the ending of Euclid's process lies in the fact that it determines a common divisor d of any two integers a, b, which is of the form $d = ax + by$ where x and y are integers. In particular, if a and b have no common divisors except units, then one may solve the indeterminate equation $ax + by = 1$ in integers x, y, whence one arrives at a demonstration of the fundamental principle of division, viz.

If two integers, a, b, have no common divisors except units, then every integer that is divisible by each is divisible by their product. For, since $ax + by = 1$ may be solved in integers x, y, any number c may be written $c = c(ax + by)$; whence, if $c = ma = nb$, we obtain $c = nb.ax + ma.by = ab(nx + my)$.

The fundamental problem in the arithmetical theory of any system of numbers is necessarily the establishment of this law of division. The more common form of the law is: "If a product be divisible by an integer a, and one factor of the product have with a no common divisors except units, then the other factor of the product is divisible by a." This form exhibits the analogy between the fundamental principle of arithmetic and that of algebra, which is: "If a product be equal to zero, and one factor of the product be finite, then the other factor of the product is equal to zero." These two principles lend themselves quite similarly in their respective subjects to the theory of the resolution of the quantities to which they apply into products of powers of irreducible factors.

---

*Norm of $a + b\sqrt{-1} = a^2 + b^2$, norm of $a + bt = a^2 - ab + b^2$.

3. After the development of the biquadratic and cubic theories, it became quite natural to expect similar results in the case of n^{ic} numbers or quantities of the form $a + bt + ct^2 + \ldots$, where a, b, c are natural numbers and t is a primitive n^{th} root of unity; but this expectation was not realized. An apparently insuperable obstacle was found in the failure of the fundamental principle of division. In 1847 Lamé gave a demonstration of the celebrated last theorem of Fermat,* based upon the properties of n^{ic} numbers. Liouville, however, pointed out that Lamé's demonstration is defective in that it assumes without proof that an n^{ic} number can be resolved, and in only one way, into a product of powers of irreducible n^{ic} numbers. Cauchy's attention was attracted to the subject by the discussion, and, failing to demonstrate, he assumed that the norm† of the remainder in the division of one n^{ic} number by another could be rendered less than the norm of the divisor. But the final result of this assumption was a *reductio ad absurdum.*

Meanwhile Kummer, Jacobi and others were at work on the generalization of the theorems of biquadratic and cubic reciprocity. Kummer thus found that the n^{ic} numbers ($n = 23$ or a higher prime) failed to conform to the fundamental law of division, and in order to overcome this difficulty he developed the theory of Ideal Primes. A synopsis of Kummer's theory, with references to his various memoirs on the subject, may be found in Smith's Report on the Theory of Numbers, B. A. Rep. 1860, pp. 120–40. The essential feature of the theory lies in the conception and definition of an ideal prime. In brief, if q be a natural prime that is resolvable into a product of true n^{ic} primes, and any n^{ic} number $f(t)$ be divisible by one of these primes, Kummer has shown that a corresponding congruence among natural numbers derivable from $f(t)$ is satisfied for the modulus q. Conversely, if q be not actually resolvable into a product of true primes, Kummer still considers it as *ideally* resolvable into a product of true primes corresponding to the congruences referred to. An ideal prime has thus, as its name implies, no actual existence among n^{ic} numbers, but one may determine whether or not an n^{ic} number $f(t)$ is divisible by such a prime by aid of the corresponding congruence, which is always actual.

4. Dirichlet next established an arithmetical theory of still more general

---

* See Smith's Report on the Theory of Numbers, B. A. Rep. 1860, p. 150.

† Norm of $a + bt + ct^2 + \ldots = (a + bt + ct^2 + \ldots)(a + bt' + ct'^2 + \ldots) \ldots$, t, t', $\ldots$ being the primitive n^{th} roots of unity.

numbers, viz. of *complex* numbers, or quantities of the form $a + bt + ct^2 + \ldots$, where a, b, c, ... are (in general) natural numbers and t is a root of an irreducible equation $t^n + a_1 t^{n-1} + a_2 t^{n-2} + \ldots = 0$, whose coefficients are natural numbers. The *norm* of a complex number $f(t)$ is the product $f(t) f(t') \ldots$, extending to all the roots t, t', ... of the given equation. Being a symmetric function of the roots, the norm is a natural number, and, in consequence, every complex number will be a divisor of some natural number. If the coefficients of a complex number be taken as indeterminate, its norm will represent a homogeneous *form*, of a certain degree, of the kind that is decomposable into linear factors. The theory of complex numbers is in reality the theory of these forms, and it is from this point of view that Dirichlet has made his very general researches upon those forms of any degree whatever which depend upon the norms of complex numbers. Dirichlet has presented his results only in a very summary manner.

Dedekind (Dirichlet's Zahlentheorie), Zolotareff (Liouv. Jour. Math. 1880), and others, have presented the theory of complex numbers from the point of view of their decomposition into prime factors. Zolotareff employs auxiliary congruences, as Kummer has done, to define the unavoidable ideal prime. Dedekind identifies any ideal complex number directly by the aggregate of all the complex numbers that it can be said to divide. For example, the complex numbers 2 and $1 + t$, pertaining to a root t of the equation $t^2 + 5 = 0$, have no actual common divisors except the units,* but they have an ideal common divisor whose square is 2, since $(1 + t)^2 = 2(-2 + t)$. Now, complex numbers of the form

$$2(a + bt) + (1 + t)(c + dt),$$

or $\quad (2a + c - 5d) + (2b + c + d)t, \quad$ or $\quad x + yt$, where $x \equiv y$ mod. 2,

constitute an assemblage of numbers each of which would be divisible by a common divisor of 2 and $1 + t$, did such exist. The (hypothetical) number that divides all numbers of the above assemblage, and those only, is Dedekind's ideal greatest common divisor of 2 and $1 + t$. The assemblage $x + yt$, $x \equiv y$ mod. 2, is the *Ideal* corresponding to this greatest common divisor of 2 and $1 + t$.

---

* Let $a + bt$ be any common divisor of 2 and $1 + t$, where a, b are natural numbers; then

$$2(1 + t) = (a + bt)^2 (x + yt), \quad \therefore\ 2(1 - t) = (a - bt)^2 (x - yt),$$
$$\therefore\ 24 = (a^2 + 5b^2)^2 (x^2 + 5y^2), \quad \therefore\ a^2 + 5b^2 = 1 \text{ or } 2,$$
$$\therefore\ a = \pm 1, \ b = 0.$$

5. A few words with regard to the latest extensions in the theory of numbers will close this summary. Dedekind and Weber (Crelle, Vol. 92) have developed an arithmetical theory of complex functions of one variable x, or quantities of the form $a + bt + ct^2 + \ldots .$, where $a, b, c, \ldots .$ are rational entire functions of x, and t is a root of the irreducible equation $a_0 t^n + a_1 t^{n-1} + \ldots . = 0$, whose coefficients are rational entire functions of x. The *ideal* complex function, which is unavoidable in this case also, is identified, after Dedekind's method, by a corresponding Ideal, or assemblage of actual complex functions.

In the same volume (92) is a memoir by Kronecker, "Grundzüge einer arithmetischen Theorie der algebraischen Grossen," which treats of the arithmetical theory of complex functions of any number of variables. The subject is treated by Kronecker as Dirichlet treats the theory of complex numbers, viz. as a theory of forms.

6. In the present memoir the foundation is laid for an arithmetical theory of numbers in general. The argument is based upon the simplest laws of algebra, and the significance of the symbols of number ($a, b, c, \ldots .$), as well as the significance of the ordinary symbols of algebra that connect them, ($=, +, -, \times, \div,$), is entirely arbitrary so long as the required fundamental laws are conserved. A necessary concomitant of the theory is the introduction of ideal integers; and this introduction is accomplished after the method of Dedekind, by the preliminary establishment of a theory of ideals. The theory of ideals here established, however, differs from Dedekind's theory in important respects, chiefly in the definition of *relatively prime* ideals, and of the *product* of two ideals, and in the exclusion of certain kinds of ideals from the theory.

Part II is devoted to the consideration of fundamental principles and definitions, to a problem and the consequences of its solution, and to turning the question of ideal solution of the problem into the question of the establishment of a given theory of ideals. The propositions in this paper, although given in the order of their dependence upon one another, are, for the most part, left without demonstration; but the demonstrations are such as may be readily supplied by the reader.

Part III is devoted to a rigorous establishment of the theory of ideals that is indicated in Part II.

PART II.

1. (Definition.) *A Universe* (Körper, Rationalitäts-Bereich) is an aggregate of numbers a, b, c, ... , such that any combination of these numbers by *addition, subtraction, multiplication* and *division* (*i. e.* any *rational* combination) is a number of the aggregate.

We here use the word "number" in the sense of a general expression to denote the objects of our attention, a, b, c, ... These objects may be themselves aggregates of other objects or numbers from which our attention is for the time being abstracted. We use the words "addition," "subtraction," "multiplication" and "division," and also the word "equal," to indicate relations and operations that are represented in the usual way and conform to the usual axioms and laws of algebra. For example: "If equals be divided by equals, the quotients are equal": "$a(b+c) = ab + ac$," "$ab.c = a.bc$," "$ab = ba$," "$a^\circ = b^\circ = c^\circ, \ldots\ldots = 1$," "$a + a = 2a$," etc.

2. (Definition.) An *Order* is an aggregate of numbers that contains every combination of its numbers by *addition, subtraction* and *multiplication* (*i. e.* every *rational entire* combination), and that also contains all the natural numbers 0, ± 1, ± 2, ± 3, ...

A universe may be regarded as divided, as to any one of its orders, into two divisions, the one consisting of numbers within the order, which may be called *integers*, the other consisting of numbers without the order, which may be called *fractions*. It is with the former numbers, or integers, that we are concerned in the present memoir.

3. (Definition.) An integer a is *divisible* by an integer b when the quotient ($b^{-1}a$ or a/b) is an integer, *i. e.* when $a = bc$, where c is an integer.

The phrase "*is* (or *are*) *divisible by*" occurs so frequently in the theory of numbers that we shall denote it by $\odot$, used by Prof. Sylvester.

4. (Theorem.) If $a \odot b$ and $b \odot c$, then $a \odot c$ and $a/c \odot b/c$.

5. (Theorem.) If a and $b \odot c$, then $ax + by \odot c$, where x, y are any integers.

6. (Definition.) A *Unit* is an integer that is a divisor of every integer.

In particular, a unit is a divisor of unity; and conversely, any integer that is a divisor of a unit is a unit. The products and quotients of units by units are also units.

7. (Definition.) *Associate integers* are integers that mutually divide each other.

Whence, the ratio of two associate integers is a unit; and if the ratio of two integers be a unit they are associates. Also, two or more associates of the same integer are associates of each other. Also, all associate integers divide, one the same integers as another, and are divisible by the same integers. We may thus select one integer out of a set of associate integers as typical of the whole, so far as questions of divisibility are concerned. A group of such integers corresponding to all sets of associate integers may be called a group of *Primary integers*, it being understood that these primary integers are always chosen (as they may be in an indefinite number of ways) so that the products of primary integers may be primary integers.

8. (Definition.) Two integers are *Relatively Prime* when every integer that is divisible by each of the two is divisible by their product.

(a). A unit is relatively prime to every integer.

(b). If a, b be relatively prime, then any two of their respective divisors are relatively prime.

(c). If each factor of one product be relatively prime to every factor of another product, then the two products are relatively prime.

E. g. let a be relatively prime to each α, β;

then if $m\alpha\beta \odot a \;\therefore\; m\alpha\beta \odot a\alpha$, or $m\beta \odot a$, [8

$\therefore\; m \odot a \;\therefore\; m\alpha\beta \odot a\alpha\beta$. Q. E. D. [8

(d). Two relatively prime integers have no common divisors except units.

9. (Problem 1.) To find a common divisor, d, of two integers, a, b, which is such that a/d, b/d are relatively prime.

We shall assume for the present that one can always find a solution of this problem in the case of any two integers a, b.[*]

10. (The fundamental principle of Division.) Two integers, a, b, that have no common divisors except units, are relatively prime.

---

[*] The term "relatively prime" used in the enunciation of Problem 1 may have various other definitions besides the one that we adopt, with the result that the fundamental principle of division may be established just as in the present instance, together with all the connected propositions. But such definition is then, for the order in question, equivalent to that of ¶ 8. On the other hand, Problem 1 is sometimes solvable according to no other definition than the one here chosen. This is the case, for example, in the order consisting of rational entire functions of an indeterminate x, whose coefficients are whole numbers only, not both whole numbers and fractions.

Euclid's process of finding the greatest common divisor of two numbers is a process for solving Problem 1 corresponding to the definition "Two integers, a, b, are relatively prime when the indeterminate equation $ax + by = 1$ may be solved in integers x, y." For Euclid's process finds, when it may be brought to an end, a common divisor, d, of a, b such that $d = ax + by$, where x, y are integers, *i. e.* such that $(a/d)\,x + (b/d)\,y = 1$.

For, let d be a solution of Problem 1;
then $\because$ d is a unit, [hyp.
$\therefore$ a, b are associates of the relatively prime integers a/d, b/d,
$\therefore$ a, b are relatively prime. Q. E. D. [7, 8b

11. (Theorem.) A solution, d, of Problem 1 is divisible by every common divisor of a, b.

For, let f be any common divisor of a, b;
then $\because ab/df \odot a/d, b/d \quad \therefore ab/df \odot ab/d^2 \quad \therefore d \odot f$. Q. E. D.

12. (Scho.) The solutions of Problem 1 form a set of associate integers which may be appropriately called *the greatest common divisors of* a, b.

13. (Problem 2.) To find a common multiple, m, of two integers, a, b, such that m/a, m/b are relatively prime.

A solution: $m = ab/d$, where d is a solution of Problem 1.

14. (Theorem.) Any solution, m, of Problem 2 is a divisor of every common multiple of a, b.

15. (Scho.) The solutions of Problem 2 form a set of associate integers which may be appropriately called *the least common multiples of* a, b.

16. (Theorem.) Problems 1 and 2 are simultaneously solvable or insolvable.

17. (Theorem.) An equation $x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots = 0$, whose coefficients are integers, can have no fractional solution.

This theorem, which depends upon 10, may be taken as a property that an order must possess before the fundamental principle of division can be established in that order. The complex numbers of the form $a + b\sqrt{-3}$, where a, b are natural numbers, furnish an example of an order that does not possess the property in question, since the fraction $(1+\sqrt{-3})/2$ is a solution of the equation $x^3 + 1 = 0$.

It is to secure this property that Dedekind defines the integer complex numbers corresponding to a root t of an irreducible equation as the rational entire functions of t that satisfy any equation whose coefficients are natural numbers, the coefficient of the highest term being unity. In accordance with this definition, the integers of the form $a + b\sqrt{-3}$ would include not only those in which a, b are whole numbers, but also those in which a, b are fractions whose denominators are powers of 2. The integers $a + b\sqrt{-3}$ would then be none other than the cubic numbers already referred to.

18. (Theorem.) If no integer be divisible by an indefinitely great power of an integer that is not a unit, and if $a^n c \odot b^n$, however large n may be, then $a \odot b$.

For, let d be a g. c. d. of a, b;
then $\because$ a^n/d^n, b^n/d^n are relatively prime, [9, 8*c*
and $\because$ $(a^n/d^n)/c \odot b^n/d^n$, [hyp.
$\therefore$ $c \odot b^n/d^n$, [where n is indefinitely great
$\therefore$ b/d is a unit, [hyp.
$\therefore$ $a \odot b$. Q. E. D.

An order of such character that its integers may have infinite powers of non-unit integers as divisors may be called a *transcendental* order. For such orders this theorem is evidently not true. The property that "if $a^n c \odot b^n$, however large n may be, then $a \odot b$" may be taken, therefore, as a property pertaining to all non-transcendental orders for which the fundamental principle of division may be established. From this property one may derive that of ¶ 17; for it is this property upon which the solutions of Problems 1 and 2 will be made to depend (III. 17). Conversely, it will be shown hereafter that if no integer be divisible by an infinite number of non-unit integers, then from the property of ¶ 17 will follow the property just stated (III. 31).

19. (Definition.) A *Homogeneous* integer is an integer no two of whose divisors are relatively prime, except one be a unit.

(*a*). Any divisor of a homogeneous integer is a homogeneous integer.

(*b*). Of two divisors of a homogeneous integer, one is a divisor of the other.

(*c*). If neither of two integers be relatively prime to a given homogeneous integer, neither are they relatively prime to each other.

(*d*). If two homogeneous integers are relatively non-prime, any two of their respective divisors are relatively non-prime, except one be a unit.

(*e*). The product of two relatively non-prime homogeneous integers is a homogeneous integer.

(*f*). Of two relatively non-prime homogeneous integers, one is a divisor of the other.

20. (Theorem.) A primary integer cannot be resolved in more than one way into a product of primary relatively prime homogeneous integers.

When an order contains *primes*, *i. e.* integers that have no divisors except their associates and the units, then these primes and any powers of these primes are homogeneous integers. We shall construct a system of integers hereafter, in which no primes exist, but in which homogeneous integers do exist.

---

21. (On the question of an *Ideal* solution of Problem 1 or 2 in cases where no actual solution exists.)

Corresponding to each integer a there is an *assemblage* of integers, a, a', a'', ... , consisting of all integers that are divisible by a. This assemblage will be called the *Primary Ideal* corresponding to a, and will be denoted by $\mathfrak{a}$.

We may note that:

(a). A primary ideal that contains a', a'' also contains $a'x + a''y$, where x, y are any integers. [5

(b). The same primary ideal corresponds to any one of a set of associate integers, and those only.

(c). We may determine the significance of products, quotients, etc., of primary ideals by the condition that if $ab = c$, then $\mathfrak{a}\mathfrak{b} = \mathfrak{c}$, and if $a/b = c$, then $\mathfrak{a}/\mathfrak{b} = \mathfrak{c}$, etc.; so that the theory of division for primary ideals corresponds to that for integers.

Now, there may be assemblages of integers that satisfy the condition (a), but that do not correspond (as above) to any integers; *e. g.* $2x + (1 + \sqrt{-5})y$ in the order $a + b\sqrt{-5}$ (I. 4). If we can join any or all of these "ideals" with the primary ideals, and extend to the whole an arithmetical theory based upon that already determined for the primary ideals, and in which Problem 1 or 2 shall always have a solution, then it is plain that this theory may be turned again into a theory of integers by regarding the non-primary ideals as corresponding to sets of associate *ideal* integers*; and that in this theory Problems 1 and 2 have always actual or ideal solutions.

It happens that there are various ways of generalizing the theory of primary ideals. Dedekind, for instance, joins with the primary ideals all other ideals. He further defines the product of two or more ideals as the assemblage of all products and sums of products of the integers of the respective factors; this being a definition that coincides with (c) when the ideals are primary (Hauptideale).

---

* By definition a unit must pertain as divisor to the assemblage of all integers of the order. As this assemblage is a primary ideal, no ideal integer can be a unit. A set of associate ideal integers consists therefore of the products of an assumed *primary* ideal integer (7) into all units of the order.

There are examples, however, that show the impossibility of reaching the utmost limits of generalization by the direct definition of the product and the consideration of all ideals. We may learn what are the most general features of the extended theory of ideals by assuming the theory of actual and ideal integers to be properly established, and deriving from that theory the theory of the corresponding, or *proper*, ideals, so as to obtain the following results:

(*d*). If m be the least common multiple of a, b, then $\mathfrak{m}$ shall consist of all integers that are common to $\mathfrak{a}$, $\mathfrak{b}$.

(*e*). If a be divisible by b, then $\mathfrak{a}$ is contained in $\mathfrak{b}$; and conversely.

(*f*). If a' be an actual integer, then shall $\mathfrak{a}'\mathfrak{b}$ be the assemblage of all products of a' into the integers of $\mathfrak{b}$, viz. $\mathfrak{a}'\mathfrak{b} = a'\mathfrak{b}$.

(*g*). The quotient $\mathfrak{a}/\mathfrak{b}$ shall consist of all integers c' such that $c'\mathfrak{b}$ is contained in $\mathfrak{a}$.

(*h*). The product $\mathfrak{a}\mathfrak{b}$ is the quotient of $a'\mathfrak{b}$ by $\mathfrak{c}$, where a' is an integer of $\mathfrak{a}$ and $\mathfrak{a}'/\mathfrak{a} = \mathfrak{c}$.

With these suggestions as to the theory of ideals, I have established its existence, using the property of ¶ 18, and the restriction that all proper ideals shall be obtainable from the primary ideals by successive derivations of least common multiples and quotients. The theory which we proceed to give rests, however, upon a different and possibly more general definition of integer ideals.

PART III.

In what follows, the integers referred to are supposed to be those of some order that is not specified except in the case of examples.

1. (Definition.) An *Ideal* of an order is such an assemblage of integers that if a', a'' be any two integers of the assemblage, then $a'x + a''y$ is an integer of the assemblage; x, y being any integers of the order.

Ideals will be represented by old English letters; thus: $\mathfrak{a}$, $\mathfrak{b}$, ... The corresponding italic letters, supplied with accents or subscripts, will denote integers of these ideals; thus: a', a'', a_1, a_2, ... are integers of $\mathfrak{a}$.

The ideal which consists of all products of an integer k into the integers of an ideal $\mathfrak{a}$ will be denoted by $k\mathfrak{a}$ or $\mathfrak{a}k$.

2. (Definition.) An ideal $\mathfrak{a}$ is *divisible* by an ideal $\mathfrak{b}$ when every integer of $\mathfrak{a}$ is an integer of $\mathfrak{b}$.

The symbol $\odot$ will be used to denote that one ideal is divisible by another, just as with integers. This symbol, when used between ideals, is thus equivalent to the words "consists of integers of."

(*a*). If $\mathfrak{a} \odot \mathfrak{b}$ and $\mathfrak{b} \odot \mathfrak{a}$, then $\mathfrak{a} = \mathfrak{b}$.
(*b*). If $\mathfrak{a} \odot \mathfrak{b}$ and $\mathfrak{b} \odot \mathfrak{c}$, then $\mathfrak{a} \odot \mathfrak{c}$.
(*c*). $a'\mathfrak{b} \odot \mathfrak{a}$; $b'\mathfrak{a} \odot \mathfrak{a}$.
(*d*). If $\mathfrak{a} \odot \mathfrak{b}$, then $k\mathfrak{a} \odot k\mathfrak{b}$.
(*e*). If $k\mathfrak{a} \odot k\mathfrak{b}$, then $\mathfrak{a} \odot \mathfrak{b}$.

The aggregate of all integers, in the order that we are considering, forms *the unit* ideal, and will be denoted by $\mathfrak{o}$. A *primary* ideal is one that consists of all integers divisible by a given integer of the order. Evidently $k\mathfrak{o}$ is the primary ideal that *corresponds* to k.

We shall make use of any integer k in a sense that will be equivalent to the use of $k\mathfrak{o}$; *i. e.* k shall be divisible by an ideal when it is an integer of that ideal, and k shall be a divisor of an ideal when it is a divisor of every integer of that ideal.

(*f*). If $\mathfrak{a} \odot k$, then $\mathfrak{a} = k\mathfrak{b}$, where $\mathfrak{b}$ is an ideal.

3. (Definition.) The *Least Common Multiple* of two or more ideals is the assemblage of all their common integers.

(*a*). The least common multiple of two or more ideals is an ideal. For if

m', m'' be common integers of $\mathfrak{a}, \mathfrak{b}, \ldots\ldots,$

then $m'x + m''y$ is a common integer of $\mathfrak{a}, \mathfrak{b}, \ldots\ldots$ Q. E. D. [1

(*b*). The least common multiple of two or more ideals is divisible by each ideal.

(*c*). An ideal that is divisible by each of two or more ideals is divisible by their least common multiple.

4. (Definition.) The *Quotient* $\mathfrak{a}/\mathfrak{b}$ of an ideal $\mathfrak{a}$ by an ideal $\mathfrak{b}$ consists of all integers k such that $k\mathfrak{b} \odot \mathfrak{a}$.

(Rem.) If $\mathfrak{a}$ be not divisible by $\mathfrak{b}$, then $\mathfrak{a}/\mathfrak{b}$ is the same as $\mathfrak{m}/\mathfrak{b}$ where $\mathfrak{m}$ is the least common multiple of $\mathfrak{a}$, $\mathfrak{b}$. For, $\because k\mathfrak{b} \odot \mathfrak{a}, \mathfrak{b}$, $\therefore k\mathfrak{b} \odot \mathfrak{m}$ or $k \odot \mathfrak{m}/\mathfrak{b}$; and conversely, if k' be any integer of $\mathfrak{m}/\mathfrak{b}$, then $\because k'\mathfrak{b} \odot \mathfrak{m} \odot \mathfrak{a}$ $\therefore k' \odot \mathfrak{a}/\mathfrak{b}$ $\therefore \mathfrak{m}/\mathfrak{b} = \mathfrak{a}/\mathfrak{b}$.

The assemblage of such integers k that $k\mathfrak{b} \odot \mathfrak{a}$ need not therefore be represented by $\mathfrak{a}/\mathfrak{b}$ when $\mathfrak{a}$ is not divisible by $\mathfrak{b}$, but by $\mathfrak{m}/\mathfrak{b}$. So far as the present investigation is concerned, the symbol $\mathfrak{a}/\mathfrak{b}$ shall have no meaning, and will not be employed, unless $\mathfrak{a} \odot \mathfrak{b}$.

(*a*). The quotient of $\mathfrak{a}$ by $\mathfrak{b}$ is an ideal.

For if c', c'' be any two integers of the quotient,

then $\because$ $c'b'$, $c''b'$ are integers of $\mathfrak{a}$, [4

$\therefore$ $c'b'x + c''b'y$ or $(c'x + c''y)\,b' \odot \mathfrak{a}$, or $(c'x + c''y)\,\mathfrak{b} \odot \mathfrak{a}$. Q. E. D.

(*b*). $\mathfrak{a} \odot \mathfrak{a}/\mathfrak{b}$.

For $\because$ $a'\mathfrak{b} \odot \mathfrak{a}$ $\therefore$ $\mathfrak{a} \odot \mathfrak{a}/\mathfrak{b}$. Q. E. D. [2*c*, 4

(*c*). If $\mathfrak{a}/\mathfrak{b} = \mathfrak{c}$, then $b'\mathfrak{c} \odot \mathfrak{a}$; *i. e.*, $b'(\mathfrak{a}/\mathfrak{b}) \odot \mathfrak{a}$.

(*d*). If $\mathfrak{a} \odot \mathfrak{b} \odot \mathfrak{c}$, then $\mathfrak{a}/\mathfrak{c} \odot \mathfrak{b}/\mathfrak{c}$ and $\mathfrak{a}/\mathfrak{c} \odot \mathfrak{a}/\mathfrak{b}$.

For if k be any integer of $\mathfrak{a}/\mathfrak{c}$,

then $\because$ $k\mathfrak{c} \odot \mathfrak{a} \odot \mathfrak{b}$ $\therefore$ $k \odot \mathfrak{b}/\mathfrak{c}$, Q. E. D. [4

and $\because$ $k\mathfrak{b} \odot k\mathfrak{c} \odot \mathfrak{a}$ $\therefore$ $k \odot \mathfrak{a}/\mathfrak{b}$. Q. E. D. [2*d*, 4

(*e*). $k\mathfrak{a}/k\mathfrak{b} = \mathfrak{a}/\mathfrak{b}$.

For let $\mathfrak{c} = k\mathfrak{a}/k\mathfrak{b}$, $\mathfrak{d} = \mathfrak{a}/\mathfrak{b}$; [2*e*

then $\because$ $d'\mathfrak{b} \odot \mathfrak{a}$ $\therefore$ $d'k\mathfrak{b} \odot k\mathfrak{a}$ $\therefore$ $\mathfrak{d} \odot k\mathfrak{a}/k\mathfrak{b} = \mathfrak{c}$, [4, 2*d*

and $\because$ $c'k\mathfrak{b} \odot k\mathfrak{a}$ $\therefore$ $c'\mathfrak{b} \odot \mathfrak{a}$ $\therefore$ $\mathfrak{c} \odot \mathfrak{a}/\mathfrak{b} = \mathfrak{d}$, [2*e*

$\therefore$ $\mathfrak{c} = \mathfrak{d}$. Q. E. D.

(*f*). $k\mathfrak{a}/k = \mathfrak{a}/\mathfrak{o} = \mathfrak{a}$.

(*g*). $k\,(\mathfrak{a}/k) = \mathfrak{a}$. (Put $\mathfrak{a} = k\mathfrak{b}$.) [2*f*, 4*f*

5. (Definition.) The *Product* $\mathfrak{a}\mathfrak{b}$ of two ideals $\mathfrak{a}$, $\mathfrak{b}$ is any ideal $\mathfrak{w}$, if it may be found, such that $\mathfrak{w}/\mathfrak{a} = \mathfrak{b}$.

(Rem.) In general there may be more than one product of two ideals, or there may be none; also, $\mathfrak{a}\mathfrak{b}$ and $\mathfrak{b}\mathfrak{a}$ may differ.

The problem before us is to show that, by considering an order whose integers satisfy a given condition, we may determine an aggregate of ideals of that order whose products are associative, commutative, unambiguous, and within the aggregate. There may perhaps be more than one such aggregate; but all are included within the aggregate of ideals, which are defined as follows:

6. (Definition.)* A *Proper* Ideal $\mathfrak{a}$ is one such that if $\mathfrak{t}k \odot \mathfrak{a}$ and $\mathfrak{t}k/\mathfrak{a} \odot \mathfrak{t}$, then $k \odot \mathfrak{a}$.

---

* Either of the following definitions of proper ideals is equivalent to this definition: "A *Proper* ideal $\mathfrak{a}$ is one such that if $\mathfrak{w}/\mathfrak{a} = \mathfrak{b}$, then $\mathfrak{w}/\mathfrak{b} = \mathfrak{a}$." "A *Proper* ideal $\mathfrak{a}$ is one such that it is the *quotient* of a primary ideal $a'\mathfrak{o}$ by some ideal $\mathfrak{b}$."

(a). If $\mathfrak{a}$ be a proper ideal, and if $k\mathfrak{t} \odot \mathfrak{a}$ and $k\mathfrak{t}/\mathfrak{a} \odot k$, then $\mathfrak{t} \odot \mathfrak{a}$.

7. (Theorem.) The least common multiple, $\mathfrak{m}$, of two or more proper ideals, $\mathfrak{a}$, $\mathfrak{b}$, ... , is a proper ideal.

For let k be any integer such that $\mathfrak{t}k \odot \mathfrak{m}$ and $\mathfrak{t}k/\mathfrak{m} \odot \mathfrak{t}$;

then $\because\ \mathfrak{t}k \odot \mathfrak{m} \odot \mathfrak{a}\ \ \therefore\ \mathfrak{t}k/\mathfrak{a} \odot \mathfrak{t}k/\mathfrak{m} \odot \mathfrak{t}$, [4$d$

$\therefore\ k \odot \mathfrak{a}$. So, $k \odot \mathfrak{b}$, ... [$\mathfrak{a}$, $\mathfrak{b}$, ... proper ideals

$\therefore\ k \odot \mathfrak{m}$. Q. E. D.

8. (Theorem.) The quotient, $\mathfrak{c}$, of a proper ideal $\mathfrak{a}$ by an ideal $\mathfrak{b}$ is a proper ideal.

For let k be any integer such that $\mathfrak{t}k \odot \mathfrak{c}$ and $\mathfrak{t}k/\mathfrak{c} \odot \mathfrak{t}$;

then $\because\ \mathfrak{t}k \odot \mathfrak{c}\ \ \therefore\ \mathfrak{t}b'k \odot b'\mathfrak{c} \odot \mathfrak{a}$, [2$d$, 4$c$

$\therefore\ \mathfrak{t}b'k/\mathfrak{a} \odot \mathfrak{t}k/\mathfrak{c} \odot \mathfrak{t}$, [4$d$, 4$e$

$\therefore\ b'k \odot \mathfrak{a}$, [$\mathfrak{a}$ a proper ideal

$\therefore\ k\mathfrak{b} \odot \mathfrak{a}\ \ \therefore\ k \odot \mathfrak{c}$. Q. E. D.

9. (Theorem.) If $\mathfrak{a}/\mathfrak{b} = \mathfrak{c}$, where $\mathfrak{b}$ is a proper ideal, then $\mathfrak{a}/\mathfrak{c} = \mathfrak{b}$.

For let k be any integer of $\mathfrak{a}/\mathfrak{c}$;

then $\because\ \mathfrak{c}k \odot \mathfrak{a} \odot \mathfrak{b}\ \ \therefore\ \mathfrak{c}k/\mathfrak{b} \odot \mathfrak{a}/\mathfrak{b} = \mathfrak{c}$, [4$d$

$\therefore\ k \odot \mathfrak{b}$ or $\mathfrak{a}/\mathfrak{c} \odot \mathfrak{b}$, [$\mathfrak{b}$ a proper ideal

and $\because\ b'\mathfrak{c} \odot \mathfrak{a}\ \ \therefore\ \mathfrak{b} \odot \mathfrak{a}/\mathfrak{c}$, [4c

$\therefore\ \mathfrak{a}/\mathfrak{c} = \mathfrak{b}$. Q. E. D.

10. (Cor.) If $\mathfrak{b}$ and $\mathfrak{c}$ be proper ideals, then $\mathfrak{b}\mathfrak{c} = \mathfrak{c}\mathfrak{b}$; *i. e.* every dividend for which $\mathfrak{b}$ is divisor and $\mathfrak{c}$ quotient is a dividend for which $\mathfrak{c}$ is divisor and $\mathfrak{b}$ quotient, and *vice versa.*

11. (Theorem.) If $(\mathfrak{w}/\mathfrak{a})/\mathfrak{b} = \mathfrak{c}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are proper ideals, then $(\mathfrak{w}/\mathfrak{c})/\mathfrak{a} = \mathfrak{b}$.

For $\because\ \mathfrak{w} \odot \mathfrak{w}/\mathfrak{a} \odot \mathfrak{c}\ \ \therefore\ \mathfrak{w}/\mathfrak{c} \odot \mathfrak{w}/(\mathfrak{w}/\mathfrak{a}) = \mathfrak{a}$. [4$b$, 4$d$, 9

Hence, let k be any integer of $(\mathfrak{w}/\mathfrak{c})/\mathfrak{a}$;

then $\because\ k\mathfrak{a} \odot \mathfrak{w}/\mathfrak{c}\ \ \therefore\ kc'\mathfrak{a} \odot \mathfrak{w}\ \ \therefore\ kc' \odot \mathfrak{w}/\mathfrak{a}$, [4, 2$d$, 4$c$

$\therefore\ k\mathfrak{c} \odot \mathfrak{w}/\mathfrak{a}\ \ \therefore\ k \odot (\mathfrak{w}/\mathfrak{a})/\mathfrak{c} = \mathfrak{b}$, [9

and $\because\ b'\mathfrak{c} \odot \mathfrak{w}/\mathfrak{a}\ \ \therefore\ b'a'\mathfrak{c} \odot \mathfrak{w}\ \ \therefore\ b'a' \odot \mathfrak{w}/\mathfrak{c}$, [4$c$, 2$d$

$\therefore\ b'\mathfrak{a} \odot \mathfrak{w}/\mathfrak{c}\ \ \therefore\ \mathfrak{b} \odot (\mathfrak{w}/\mathfrak{c})/\mathfrak{a}$,

$\therefore\ (\mathfrak{w}/\mathfrak{c})/\mathfrak{a} = \mathfrak{b}$. Q. E. D.

12. (Cor.) The existence of a product of two proper ideals, $\mathfrak{a}$ and $\mathfrak{b}$, depends upon the existence of an ideal $\mathfrak{w}$ such that $\mathfrak{w} \odot \mathfrak{a}$ and $\mathfrak{w}/\mathfrak{a} \odot \mathfrak{b}$ [viz.

from $(\mathfrak{w}/\mathfrak{a})/\mathfrak{b} = \mathfrak{c}$ one finds $\mathfrak{w}/\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ (11)]; and if $\mathfrak{w}$ be a proper ideal, then the corresponding product, $\mathfrak{a}\mathfrak{b}$, is a proper ideal. [8

13. (Cor.) If $\mathfrak{a}$, $\mathfrak{b}$ and $(\mathfrak{w}/\mathfrak{a})/\mathfrak{b} = \mathfrak{c}$ be proper ideals, then

$$\mathfrak{w}/\mathfrak{a} = \mathfrak{b}\mathfrak{c} = \mathfrak{c}\mathfrak{b},\ \mathfrak{w}/\mathfrak{b} = \mathfrak{a}\mathfrak{c} = \mathfrak{c}\mathfrak{a},\ \mathfrak{w}/\mathfrak{c} = \mathfrak{a}\mathfrak{b} = \mathfrak{b}\mathfrak{a},\ (\mathfrak{w}/\mathfrak{a})/\mathfrak{b} = \mathfrak{w}/\mathfrak{a}\mathfrak{b} = \mathfrak{c}, \ldots.;$$

i. e. $\mathfrak{a}.\mathfrak{b}\mathfrak{c} = \mathfrak{a}.\mathfrak{c}\mathfrak{b} = \mathfrak{b}.\mathfrak{c}\mathfrak{a} = \mathfrak{b}.\mathfrak{a}\mathfrak{c} = \mathfrak{c}.\mathfrak{a}\mathfrak{b} = \mathfrak{c}.\mathfrak{b}\mathfrak{a} = \mathfrak{a}\mathfrak{b}.\mathfrak{c}, \ldots.$

14. (Cor.) Multiplication among proper ideals is associative and commutative; *i. e.* every ideal that is a product of given proper ideals corresponding to one arrangement and association of the factors is also a product corresponding to any other arrangement and association of the factors.

15. (Theorem.) If $\mathfrak{a}/\mathfrak{b} \odot \mathfrak{a}/\mathfrak{c}$, where $\mathfrak{b}$ is a proper ideal, then $\mathfrak{c} \odot \mathfrak{b}$.

For let $\mathfrak{a}/\mathfrak{c} = \mathfrak{v}$;

then $\because c'\mathfrak{v} \odot \mathfrak{a} \quad \therefore \mathfrak{c} \odot \mathfrak{a}/\mathfrak{v}$,

and $\because \mathfrak{a} \odot \mathfrak{a}/\mathfrak{b} \odot \mathfrak{v} \quad \therefore \mathfrak{a}/\mathfrak{v} \odot \mathfrak{a}/(\mathfrak{a}/\mathfrak{b}) = \mathfrak{b}$, [4*d*, 9

$\therefore \mathfrak{c} \odot \mathfrak{a}/\mathfrak{v} \odot \mathfrak{b}$. Q. E. D.

16. (Cor.) If $\mathfrak{a}/\mathfrak{b} = \mathfrak{a}/\mathfrak{c}$, where $\mathfrak{b}$ and $\mathfrak{c}$ are proper ideals, then $\mathfrak{b} = \mathfrak{c}$.

17. (Definition.) A *System* is an order whose integers $a, b, c, \ldots.$ are such that if $a^n c \odot b^n$, however large n may be, then $a \odot b$. [Compare Part II, 18

The propositions that follow have reference only to integers of a system.

18. (Lemma.) If $k\mathfrak{t} \odot a\mathfrak{t}$, then $k \odot a$.

For $\because k\mathfrak{t} \odot a\mathfrak{t} \quad \therefore kt' = at_1$;

so $kt_1 = at_2,\ kt_2 = at_3, \ldots.,\ kt_{n-1} = at_n,$ [$n = 1, 2, 3, \ldots.$ *ad inf.*

$\therefore k^n t' t_1 t_2 \ldots. t_{n-1} = a^n t_1 t_2 \ldots. t_n \quad \therefore k^n t' = a^n t_n,$

$\therefore k^n t' \odot a^n$, however large n may be; $\therefore k \odot a$. Q. E. D. [17

19. (Cor.) If $k\mathfrak{v} \odot a\mathfrak{t}$ where $\mathfrak{t} \odot \mathfrak{v}$, then $k \odot a$.

For $\because \mathfrak{t} \odot \mathfrak{v} \quad \therefore k\mathfrak{t} \odot k\mathfrak{v} \odot a\mathfrak{t} \quad \therefore k \odot a$.

20. (Cor.) A primary ideal is a proper ideal.

For let $a\mathfrak{o}$ be a primary ideal, and let k be an integer such that $\mathfrak{t}k \odot a$ and $\mathfrak{t}k/a \odot \mathfrak{t}$;

then $\because \mathfrak{t}k/a \odot \mathfrak{t} \quad \therefore \mathfrak{t}k \odot \mathfrak{t}a$, [4*g*

$\therefore k \odot a$. Q. E. D.

21. (Theorem.) If $\mathfrak{a} \odot \mathfrak{b}$, then $k\mathfrak{a}/\mathfrak{b} = k(\mathfrak{a}/\mathfrak{b})$.

For let $\mathfrak{u} = k\mathfrak{a}/\mathfrak{b},\ \mathfrak{v} = \mathfrak{a}/\mathfrak{b}$;

then $\because u\mathfrak{b}' \odot k\mathfrak{a}$ and $\because \mathfrak{a} \odot \mathfrak{b} \ \therefore u' \odot k$, [19

$\therefore (u'/k)\mathfrak{b} \odot \mathfrak{a} \ \therefore u'/k \odot \mathfrak{a}/\mathfrak{b} \ \therefore \mathfrak{u} \odot k(\mathfrak{a}/\mathfrak{b}) = k\mathfrak{v}$, [2*e*, 2*d*

and $\because v'\mathfrak{b} \odot \mathfrak{a} \ \therefore kv'\mathfrak{b} \odot k\mathfrak{a} \ \therefore k\mathfrak{v} \odot k\mathfrak{a}/\mathfrak{b} = \mathfrak{u}$,

$\therefore \mathfrak{u} = k\mathfrak{v}$. Q. E. D.

22. (Cor.) There exists, corresponding to any two proper ideals $\mathfrak{a}$ and $\mathfrak{b}$, a proper ideal that is their product.

For $\because a'b'\mathfrak{o}$ is a proper ideal divisible by $\mathfrak{a}$,

and $\because a'b'/\mathfrak{a} = b'(a'/\mathfrak{a}) \odot \mathfrak{b}$, [21, 2*c*

$\therefore a'b'$ by $(a'b'/\mathfrak{a})/\mathfrak{b}$ is a proper ideal $\mathfrak{a}\mathfrak{b}$. Q. E. D. [12

23. (Cor.) If $\mathfrak{a}$ be a proper ideal, then $k\mathfrak{a}$ is the proper ideal $k\mathfrak{o}/\mathfrak{a}$.

24. (Theorem.) If $\mathfrak{a}/\mathfrak{c} \odot \mathfrak{b}/\mathfrak{c}$, where $\mathfrak{b}$ is a proper ideal, then $\mathfrak{a} \odot \mathfrak{b}$.

For let k be any integer of $b'\mathfrak{a}/\mathfrak{b}$;

then $\because k\mathfrak{b} \odot b'\mathfrak{a} \odot \mathfrak{c}$ and $\because \mathfrak{a} \odot \mathfrak{c},\ \mathfrak{b} \odot \mathfrak{c} \ \therefore k(\mathfrak{b}/\mathfrak{c}) \odot b'(\mathfrak{a}/\mathfrak{c})$, [21, 4*d*

and $\because \mathfrak{a}/\mathfrak{c} \odot \mathfrak{b}/\mathfrak{c} \ \therefore k \odot b'$, *i. e.* $b'\mathfrak{a}/\mathfrak{b} \odot b'$, [19

$\therefore \mathfrak{a} \odot \mathfrak{b}$. Q. E. D. [6*a*

25. (Cor.) If $\mathfrak{a}/\mathfrak{c} = \mathfrak{b}/\mathfrak{c}$, where $\mathfrak{a}$ and $\mathfrak{b}$ are proper ideals, then $\mathfrak{a} = \mathfrak{b}$.

26. (Recapitulation.) The proper ideals of a system are duplicated by multiplication amongst themselves (22); multiplication and division conform to the ordinary rules of algebra (14); of the three related elements, *product*, *divisor*, *quotient*, any two being given, the other is unambiguously determined (4, 25, 16), while $\mathfrak{a} \odot \mathfrak{b}$ implies that $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, and conversely, wherein $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ are proper ideals.

27. (Definition.) Two ideals are Relatively Prime when every ideal* that is divisible by each is divisible by their product.

28. (Solution of Problem 2.) If $\mathfrak{m}$ be the least common multiple of the proper ideals $\mathfrak{a}$ and $\mathfrak{b}$, then $\mathfrak{m}/\mathfrak{a}$ and $\mathfrak{m}/\mathfrak{b}$ are relatively prime.

For let k be any integer divisible by $\mathfrak{m}/\mathfrak{a}$ and $\mathfrak{m}/\mathfrak{b}$,

then $\because k\mathfrak{a},\ k\mathfrak{b} \odot \mathfrak{m} \ \therefore k\mathfrak{a}\mathfrak{b} \odot \mathfrak{m}\mathfrak{a},\ \mathfrak{m}\mathfrak{b} \ \therefore k\mathfrak{a}\mathfrak{b}/\mathfrak{m} \odot \mathfrak{a},\ \mathfrak{b}$,

$\therefore k\mathfrak{a}\mathfrak{b}/\mathfrak{m} \odot \mathfrak{m} \ \therefore k \odot \mathfrak{m}^2/\mathfrak{a}\mathfrak{b}$. Q. E. D.

(Conclusion.) If the primary divisor, *actual* or *ideal*, of all integers of an integer ideal $\mathfrak{a}$, and those only, be denoted by a, then such system of actual and ideal integers fulfils the fundamental principle of division. Q. E. D. [II, 16, 9, 10

---

* "Proper" or "primary ideal" may be substituted for the word "ideal" in this definition without loss of generality.

29. (Theorem.) If $\mathfrak{b}$ be a proper ideal and $\mathfrak{a}^n\mathfrak{c} \odot \mathfrak{b}^n$, however large n may be, then $\mathfrak{a} \odot \mathfrak{b}$.

For let $b'/\mathfrak{b} = \mathfrak{d}$;

then $\because\ a'^n c' \odot \mathfrak{a}^n\mathfrak{c} \odot \mathfrak{b}^n$,

$\therefore\ (a'd')^n c' \odot (d'\mathfrak{b})^n \odot b'^n\ \therefore\ a'd' \odot b'$, [17

$\therefore\ \mathfrak{a} \odot b'/\mathfrak{d} = \mathfrak{b}$. Q. E. D.

30. (Cor.) No ideal is divisible by an indefinitely great power of any other proper ideal than $\mathfrak{o}$.

For if $\mathfrak{c},\ = \mathfrak{o}^n\mathfrak{c},\ \odot \mathfrak{b}^n$, however large n may be,

$\therefore\ \mathfrak{o} \odot \mathfrak{b}\ \therefore\ \mathfrak{b} = \mathfrak{o}$. Q. E. D.

31. (Theorem). Any order is a system in which no ideal is divisible by an infinite number of ideals, and in which no fractional number a/b satisfies an equation $x^n + a_1x^{n-1} + \ldots\ldots a = 0$, whose coefficients, $a_1, \ldots\ldots a_n$, are integers of the order.

For let $a^n c \odot b^n$; *i. e.*, let $cx = c(a/b)$, $cx^2, \ldots\ldots cx^n$ be integers, however large n may be. From the integers $cx, \ldots\ldots$ form the series of ideals (cx, cx^2), $(cx, cx^2, cx^3), \ldots\ldots (cx, cx^2, \ldots\ldots cx^n)$, where, to explain the notation, the first ideal consists of all integers of the form $cx.u + cx^2.v$, u, v being any integers of the order; then

$\because$ the first of the infinite number of ideals so formed is divisible by all the others,

$\therefore$ the series consists of a finite number of different ideals, [hyp.

$\therefore$ by taking s large enough we shall have

$$(cx, cx^2, \ldots\ldots cx^s) = (cx, cx^2, \ldots\ldots cx^t), \text{ where } t < s;$$

$\therefore\ cx^s = cxu_1 + cx^2u_2 + \ldots\ldots cx^tu_t$, where $u_1, \ldots\ldots u_t$ are integers of the order,

$\therefore\ x^s - u_tx^t - u_{t-1}x^{t-1} - \ldots\ldots - u_1x = 0$,

$\therefore$ x is not a fractional number; *i. e.*, $a \odot b$. Q. E. D. [hyp.

32. (Definition.) The *Compound* of two or more ideals, $\mathfrak{a}, \mathfrak{b}, \ldots\ldots$ is the ideal consisting of all products, $a'b', \ldots\ldots$ between the integers of the given ideals and the sums of those products.

The compound of $\mathfrak{a}, \mathfrak{b} \ldots\ldots$ will be denoted by $\mathfrak{a} \times \mathfrak{b} \times \ldots\ldots$; the compound of $\mathfrak{a}$, taken n times, by $[\mathfrak{a}]^n$.

$$(a).\ \mathfrak{a}\times\mathfrak{b}\times\mathfrak{c} = \mathfrak{b}\times\mathfrak{a}\times\mathfrak{c} = \ldots\ldots = \mathfrak{a}\times(\mathfrak{b}\times\mathfrak{c}) = \mathfrak{b}\times(\mathfrak{a}\times\mathfrak{c}) = \ldots\ldots;$$

$$[\mathfrak{a}\times\mathfrak{b}]^n = [\mathfrak{a}]^n \times [\mathfrak{b}]^n.$$

(*b*). The compound of two or more ideals is divisible by each of the ideals.

(*c*). The compound of divisor and quotient is divisible by the dividend; also, the compound of any number of ideals is divisible by any product of those ideals.

(*d*). If $\mathfrak{a} \odot \mathfrak{b}$ and $\mathfrak{x} \odot \mathfrak{y}$, then $\mathfrak{a} \times \mathfrak{x} \odot \mathfrak{b} \times \mathfrak{y}$; in particular $[\mathfrak{a}]^n \odot [\mathfrak{b}]^n$.

(*e*). If there be any ideal $\mathfrak{c}$ such that $\mathfrak{c}/\mathfrak{a} = \mathfrak{b}$, then $\mathfrak{a} \times \mathfrak{b}$ is such an ideal.

For $\because \mathfrak{a} \times \mathfrak{b} \odot \mathfrak{c} \quad \therefore \mathfrak{a} \times \mathfrak{b}/\mathfrak{a} \odot \mathfrak{c}/\mathfrak{a} = \mathfrak{b}$, [32*c*, 4*d*, hyp.
and $\because \mathfrak{b} \times \mathfrak{a} \odot \mathfrak{a} \times \mathfrak{b} \quad \therefore \mathfrak{b} \odot \mathfrak{a} \times \mathfrak{b}/\mathfrak{a}$, [4
$\therefore \mathfrak{a} \times \mathfrak{b}/\mathfrak{a} = \mathfrak{b}$. Q. E. D.

(*f*). The product of two or more proper ideals may be obtained by compounding them, when such compound is a proper ideal.

(*g*). If $\mathfrak{b}$ be a proper ideal and $[\mathfrak{a}]^n \times \mathfrak{c} \odot [\mathfrak{b}]^n$, however large n may be, then $\mathfrak{a} \odot \mathfrak{b}$.

For let $b'/\mathfrak{b} = \mathfrak{d}$;

then $\because a'^n c' \odot [\mathfrak{a}]^n \times \mathfrak{c} \odot [\mathfrak{b}]^n$, [hyp.
$\therefore (a'd')^n c' \odot [d'\mathfrak{b}]^n \odot b'^n \quad \therefore a'd' \odot b'$, [32*a*, 32*c*, 17
$\therefore \mathfrak{a} \odot b'/\mathfrak{d} = \mathfrak{b}$. Q. E. D.

CORNELL UNIVERSITY, June, 1886.